Exploring a New World of Identity with Identity 2.0 based Solutions

Wade Fagen
University of Illinois at Urbana-Champaign
201 N. Goodwin Ave.
Urbana, IL 61801
wfagen2@uiuc.edu

Karrie Karahalios
University of Illinois at Urbana-Champaign
201 N. Goodwin Ave.
Urbana, IL 61801
kkarahal@cs.uiuc.edu

ABSTRACT

On the Internet today, account registration is nearly always a requirement to interact with any website in a meaningful way. Each digital identity a user creates is a new and completely disjoint identity from all other existing digital identities of the user. These traditional identities, Identity 1.0 identities, are site-centric and centralized. Alternatively, Identity 2.0 identity solutions are completely decentralized and user-centric.

This paper presents four different examples of user interaction using Identity 2.0 based solutions that weren't possible within a traditional identity framework: greylisting, identity multiplexing, user-centric privacy, and site preregistration. To understand the examples further, two applications using aspects of the examples provided were developed and deployed on the Internet for public use. Moreover, a third prototype was developed to further understand how users interact within an Identity 2.0 based Internet. Through the study of server logs and informal user studies, two key observations were observed regarding general user patterns of users authenticating themselves within a new identity framework.

Categories and Subject Descriptors

H.5.2 [**Information interfaces and presentation (e.g., HCI)**]: Miscellaneous

General Terms

Identity 2.0, OpenID, Yadis, Greylisting, Website Preregistration, User-Centric Privacy, Identity Multiplexing

Keywords

Identity management, privacy, user-centric technologies, OpenID

1. INTRODUCTION

As a user browses from site to site on the Internet, the user is nearly always required to create a new account on each site if he or she would like to interact with a website in any meaningful way. At a weblog, the desired user interaction may be as simple as a comment to a posting; at a site providing finical information, the interaction could be the creation of a portfolio to manage their holdings; and at a website managing a corporate project, the interaction may be posting presentation slides or technical documents. If the user created an account at each of these sites, he or she has created a number of completely distinct user identities not by a matter of choice but by matter of the requirement of the site. As the number of sites the user has accounts on increases, the probability that the user has used the same username/password combination also increases, allowing a malicious site to potentially interact with other (otherwise trustworthy) sites because the malicious site has gained the username/password combination through the user's registration [24].

These traditional identities, which will be referred to in this paper as Identity 1.0 identities, are centralized, site-specific, and the privacy of the identity is only as good as the privacy of the site storing the identity. Alternatively, Identity 2.0 identities provide a decentralized, user-specific means of authenticating an identity to a web service without sharing any additional authentication information (such as a password) to the site requesting the authentication of a username other than the username itself. During the past couple of years, a handful of Identity 2.0 identity solutions have emerged from communities throughout the Internet [8, 10, 11, 17, 20, 21]. An overview of both cross-site (so called "single sign-on") Identity 1.0 solutions (such as the Microsoft .NET Passport [18]) and Identity 2.0 solutions (such as OpenID [21]) will be provided in Section 2.

Having a user-centric digital identity framework, this paper examines a number of interesting and different services websites can provide using Identity 2.0 solutions that were not feasible while using Identity 1.0 solutions. Examples of this range from account pre-creation (a personalized experience is set up for a user even before the user has gone to a website) to a user-centric privacy model (where the user may choose to authenticate by means other than a password). These examples, along with others, are discussed in Section 3.

To begin to understand how users interact with Identity 2.0 solutions, a number of the examples presented in Section 3 were implemented in web-based solutions that were

released onto the Internet. On such example is the uNorron project (http://unorron.com/). As part of a third party tool for a web-based MMOG called Norron [14], uNorron is an information management solution that allows for members of kingdoms within the web-based game Norron. Through OpenID authentication, users playing Norron are able to share in-game information with other kingdom members without sharing a password with uNorron and, also, without the threat of non-kingdom members accessing the information. The uNorron project is presented in detail in Section 4.1 while another project, FBOpenID (allows OpenID authentication through the Facebook API), is presented in Section 4.2.

Through the development of Identity 2.0 based applications, a number of interesting characteristics were observed by the users of the applications. One of the most significant observations was the apparent concern over the security of the OpenID authentication process, as a login to a site is no longer a username and a password box but simply a username box. Specifically, many users expressed concern and confusion over how a single login box prevents someone from logging in as their own identity. Section 5 presented this and other user reactions to using OpenID in an uncontrolled, Internet situation.

This goal of this paper isn't to promote Identity 2.0 identities as an all around better identity solution than Identity 1.0 identities, but provide interesting usage and observations over the use of Identity 2.0 identities in place of Identity 1.0 identities. In Section 6, this paper presents a vast discussion of what we see as interesting projects using Identity 2.0 identities. Finally, this paper and the results found throughout the paper are recapped in Seciton 7.

2. PREVIOUS WORK

As one of the most basic elements of being human, identity and identity management have been thoroughly researched across nearly all areas of research [2, 3, 9, 19]. Even the concept of digital identity has been so critical to a multitude of fields that there are numerous wide-ranging articles exploring numerous aspects of digital identity [15]. Of all of the previous work on the field of identity, this paper will focus on the concept that has been established in recent literature known as single sign-on (SSO) [1, 22] in Section 2.1. With the understanding of the vast collection of definitions of what SSO has become to mean, Section 2.2 examines a number of Identity 1.0-based solutions that have attempted to achieve SSO in different regards. Finally, previous work on Identity 2.0 identity solutions is presented alongside our justification to use OpenID in our implementations.

2.1 Single Sign-On

The term Single Sign-On (SSO) has existing in literature for over a decade [1] and has taken on a variety of meanings. From the original works of having a single global login (similar to the goals of the .NET framework), to a more realistic view of having a unified session based login throughout a series of services such as in CorSSO [15], SSO has nearly always been about a single username and password to authenticate in a cross-site means.

In the content of Identity 2.0, SSO has the same meaning but reaches to a different end. Rather than attempting to achieve an environment where a user would only have to login once, Identity 2.0 provides for a single globally unique identifier that allows the user to login at any site. That is, on an Internet completely using Identity 2.0 technologies, a user would need to login at every site, but he or she can log in at every site with the same username via the exact same process. This small but critical difference will be discussed further in Section 2.3.

2.2 Identity 1.0

As discussed in the introduction of this paper, Identity 1.0 identity solutions can be seen all throughout the Internet at nearly every webpage that allows any means of meaningful user interaction. However, one Identity 1.0 solutions is most notable due to its aim to achieve a global proprietary identity scheme: Microsofts .NET Passport (now called Windows Live ID). A number of publications has looked at the risks and benefits of wide-scale adoption of such a service [18], and Microsoft is pushing forward with services such as CardSpace, a built-in component of Windows Vista [7].

Several other players have also launched SSO products, such as Novell, IBM, and others [25]. However, the target markets of these SSO products are at an enterprise level and not at an Internet level. Moreover, their requirements of a centralized server in these products also make these products site-centric rather than user-centric as an Identity 2.0 solutions is required to be.

2.3 Identity 2.0

In our final section for analysis of the existing work, we will examine a number of different glasswork efforts that have lead to a growing number of Identity 2.0 identity solutions. One of the first solutions, sxip [8], was a single sign-on Identity 2.0 solution built by Sxip Identity Corporation. Having gone through two versions, sxip has recently merged with OpenID in an attempt to unify the Identity 2.0 framework.

Similar to sxip, a technology that was universally known by the acronym LID for Light-Weight Identity was developed by a bottom-up effort to create a simple but powerful technology that empowers individuals to keep control over and manage their on-line digital identities [10]. In the Summer of 2005, Brad Fitzpatrick (the creator of OpenID) and key players from the company behind LID, NetMesh, met together and created a new framework for digital interoperable identity management: Yadis [17].

In the simplest terms, Yadis is self-proclaimed as "The Identity and Accountability Foundation for Web 2.0". Yadis provides a framework to specify different authentication mechanisms - be it OpenID, LID, or inames. Moreover, since Yadis is completely XML based, Yadis will be able to expand for to encapsulate future technologies if necessary.

One of the critical technologies in Yadis is the technology of OpenID [20]. Developed by Brad Fitzpatrick in July 2005, OpenID uses a URL as a globally unique public identifier for a user. Due to the adoption of OpenID by Livejournal, Movable Type, and others, OpenID is the most widely adopted Identity 2.0 technology. A previous paper explains the technical details of OpenID [21], while a simple overview is provided for readers of this paper in Seciton 3.3.

3. SERVICES USING IDENTITY 2.0

In the years and years of studies over identity management, vast reaching ideas have been studied on how to

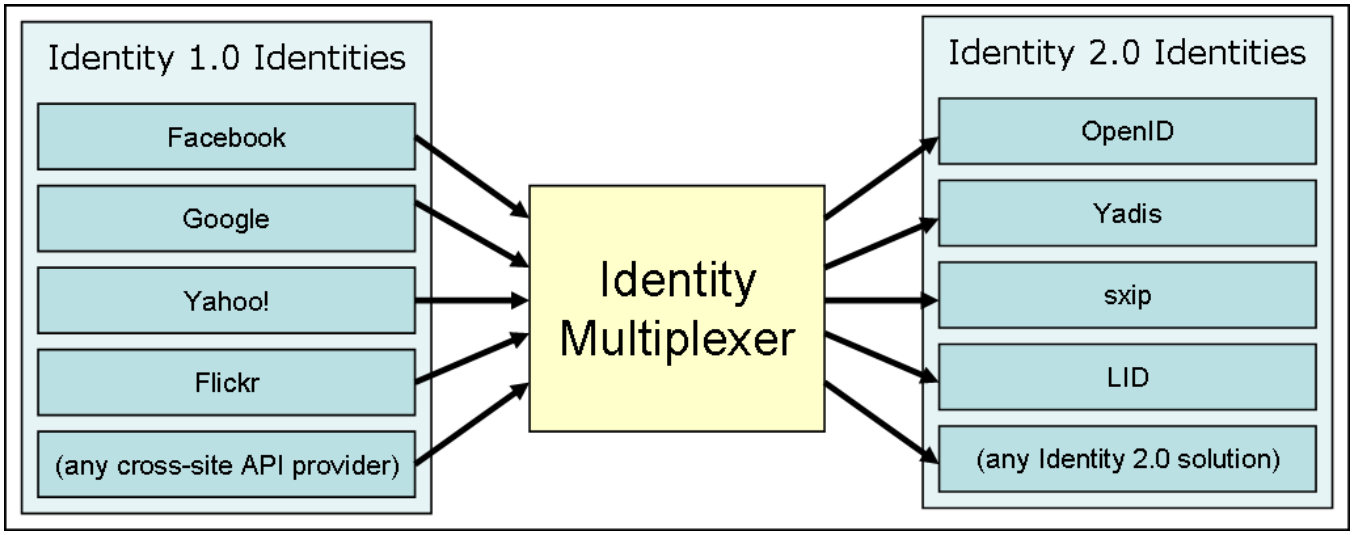

Figure 1: A diagram showing the possiblities of an identity multiplexer using any Identity 1.0 identity with a supporting API to log into any one of the many existing Identity 2.0 solutions.

streamline a user's experience through multiple websites. As discussed in the previous section, a vast majority of this literature has focused on a centralized server and applications ran within a framework mandated by that central server. However, with the growing adoption of Identity 2.0 identities, many of these ideas can be revisited, expanded upon, and extended to fit within a cross-site user-centric framework allowing for the user to have complete control over his or her identity. This section presents a collection of just a few of the technological advances in identity management that could be seen with the wide-spread adoption of Identity 2.0 identity solutions.

As one of the most pressing issues on the Internet today, the ever increasing presence of spam will be the focus of the first service examined in this section. This service, the concept of greylisting [12], when applied with Identity 2.0 identities allows for a site to both whitelist a username to allow him or her to interact with the site without needing to know anything more than the user's username and blacklist an IP or other address of a known spammer.

Following greylisting, we go on to present the idea of identity multiplexing in Section 3.2, where multiple Identity 1.0 solutions may be tied with multiple Identity 2.0 solutions at a single website. To examine the practicality of the idea, we present a small-scale Internet-based identity multiplexing implementation in Section 4.2.

Since the concept of privacy goes hand and hand with the concept of identity, Section 3.3 presents how different implementations of Identity 2.0 authentication schemes allows for a user to choose exactly how much security and privacy a user desires with each of his or her identities. Finally, since identities can be shared from site to site without the need to share private information such as passwords, sites using Identity 2.0 identity solutions can "pre-register" a user so that when the user visits this new site, the new site is already pre-customized for the user.

3.1 Greylisting

Throughout the Internet, the existence of spam has become so prevalent that sites will go to any length to prevent and eliminate spam [12]. Moreover, the research community is constantly proposing spam-mitigating technologies attempting to stop the spammer in their tracks [12]. However, current technologies of attempting to detect a spammer has generally failed or has been broken within just a matter of days [12] (for example, Human Interactive Proofs (HIPs) / CAPTICAs attempt to prevent a spammer from registering, but recent research suggest that computers can out perform humans on even the best generated HIPS [6]). To that end, there has been recent work on a new concept called "greylisting".

The basic idea behind greylisting is to combine the best aspects of both whitelisting and blacklisting. Currently, the term "greylisting" has been only used in the context of e-mail by exploiting the SNTP protocol to require the sender of the e-mail to send the e-mail twice before it is received by the user [12]. However, with the creation of a globally unique non-private user identifier, user names can now be shared on a whitelist allowing for a site to instantly trust an otherwise unknown user.

Unlike traditional whitelists that attempt to collect a list of trusted sites, greylisting in Identity 2.0 solutions benefit most from implementing a specific type of whitelists: a social whitelist. Introduced in literature in the content of e-mails, Garriss et al [12] presented the whitelisting in a friend-of-a-friend [5] content. Rather than replying on e-mail, Identity 2.0 supporting applications may collect a list of users it currently trusts and publish that list of users for other Identity 2.0 supporting applications to consume and use to the benefit of the application.

In the content of a blog, this social whitelist could be simply a list of users who have left at least five significant, non-spam comments. Clearly, this metric doesn't need to be concrete and may be site-specific - a corporation may whitelist all users who have an OpenID derived from their domain name (such as http://*.openid.net/). In fact, as of the publication of this paper, one website has already published a social whitelist for other applications to consume [23]. That

author of the website, Simon Willison, advocates a system where human interaction would be required before a blog comment would appear if the user doesn't appear on his social whitelist.

While social whitelisting alone is a step toward reducing spam, the years of work in blacklisting has proven to slow the work of spammers in numerous instances [12]. To that end, we propose combining the works of both whitelisting and blacklisting into a nbew type of greylisting. In a greylisting system, a user would be allowed to interact without restriction if he or she is on the whitelist, a user would be able to interact with limited restriction is he or she is on nether the whitelist or blacklist, and a user on the blacklist would be able to interact with only strictly limited restrictions. That way, a level of user trust is introduced into the system, allows for "good" users to interact freely, and also allows for a blacklisted user to move toward being removed from the blacklist rather than simply being banned from a site or application.

Moving beyond greylisting, the next section presents the concept of identity multiplexing alongside an application that moves toward allowing for identity multiplexing.

3.2 Identity Multiplexing

Much like Identity 1.0 solutions, there are a number of different Identity 2.0 solutions available for both users and developers. Many of theses solutions were presented in Section 2.3, where each Identity 2.0 solution exhibited some similar characteristics but were largely incompatible with each other. To overcome the user confusion of multiple competing protocols, we present the idea of identity multiplexing.

A site or application that provides for identity multiplexing is simply a site or application that allows for login via multiple Identity 1.0 providers to a single account that can be verified by multiple Identity 2.0 protocols. For example, a user may be able to log into a website, idmux.com, through his or her Facebook login, his or her Google login, his or her Yahoo! Login, or any other Identity 1.0 login service that supports cross-site authentication via some publicly available API. After creating some username, such as "amy.idmux.com", that user may not validate "amy.idmux.com" through any supported Identity 2.0 protocol. Figure 1 presents a visual description of the identity multiplexing process.

To begin to understand how users will interact with this idea, we implemented a working small-scale identity multiplexer for multiplexing a Facebook login with both OpenID and Yadis. The implementation, FBOpenID, is discussed in detail in Section 4.2.

3.3 User-Centric Privacy

As users take increasing control of their identity, the issue of privacy is also passed onto the user. In the OpenID protocol, a user logs into an OpenID-supporting site with a "claimed identity". The OpenID-supporting site then verifies the claimed identity with the user's "homesite", the web site that is tasked to prove that the identity belongs to the user. At the homesite, it is up to the user (if the user created his or her own homesite) or the provider of the homesite (if the user uses an Identity 2.0 provider) to authenticate the user by any means. Traditionally, this has been done with just a password. For example, FBOpenID (introduced in the previous section), uses a user's Facebook login to authenticate their Identity 2.0 identity. However, passwords have historically been easily phished [24] and rely on a user being extremely observant.

Since Identity 2.0 solutions no long rely on a centralized server for identification, each individual site can exploit site-specific resources for the authentication of users. For example, a corporation may set up an Identity 2.0 homesite that only allows for authentication of the identity when the request comes from within the company firewall. Likewise, a user may choose to only allow for authentication when his or her IP address is some specific IP address or within a specific range of IP addresses. The possibilities of user-centric privacy models are endless and rely only upon the user's imagination and implementation of such privacy models.

In evaluating one of these examples further, we created a prototype of an IP address regulated authentication system where a user would have to provide strong credentials to login when he or she accesses his or her homesite from outside his or her university's IP address range. Otherwise, when accessing his or her homesite form with the range, the user would only have to provide weak credentials. The system, MeIdentity, is explained in detail within the implementation section of this paper in Section 4.3.

3.4 Cross-site Pre-Registration

Having discussed greylisting, identity multiplexing, user-defined and user-centric privacy models, we move on to discuss our final service that can vastly improve the user experience on the web. Using the characteristic of Identity 2.0 identity solutions discussed earlier of a globally unique public username that can be shared without any information other than the username, the ability to pre-register a user to a specific website based on his or her preferences or usage of another website is now feasible. The only limitation of this cross-site service would be the availability of public information. That is, preferences that a user sees on some website only when logged in and is only manifested in that user's session could, obviously, not be read by another website that is otherwise completely disjoint from the original site.

Imagine a world where each comment you make on a blog post already knew what formatting tags you preferred to use, already knew what screen name you preferred to use, and more. By extending this further, frameworks could be developed to transfer data between two different sites about a user without needing to exchange any personal information about the user themselves. For example, if a user posted a large percentage of his or her posts in the anthropology section of a site's forum, a site may wish to customize their interface for that user to reflect their anthropological interests.

As more and more sites use Identity 2.0 identity solutions, we believe it will be clear that cross-site profile gathering will be a critical field of study. We discuss possibly projects to realize these effects in our Future Works section.

4. IMPLEMENTATIONS USING OPENID

Throughout all of Section 3, we discussed a number of different and interesting uses of identities under the new context of identity management available with Identity 2.0 identity solutions. Throughout that section, we referenced a number of projects that we have prototyped and, in all but

one case, completed a full implementation that was deployed on the Internet for public use. In each of these implementations, the Identity 2.0 solution used was OpenID as it has become the most prevalent Identity 2.0 solution available on the Internet. Moreover, FBOpenID, the implementation to study identity multiplexing, also used Yadis to examine the benefits of identity multiplexing.

The first of the three projects presented is an information manager for an online massively multiplayer game by Nathaniel Johnston entitled Norron [14]. A complete description of our information manager implementation is available in Seciton 4.1. The next project, introduced in Section 3.2 and earlier in this introduction of implementations, FBOpenID, implements a small-scale identity multiplexer that allows users to use their Facebook login as the authentication mechanism to their Identity 2.0 identity. Finally, MeIdentity, examines user-centric security models and is discussed in Seciton 4.3.

4.1 uNorron

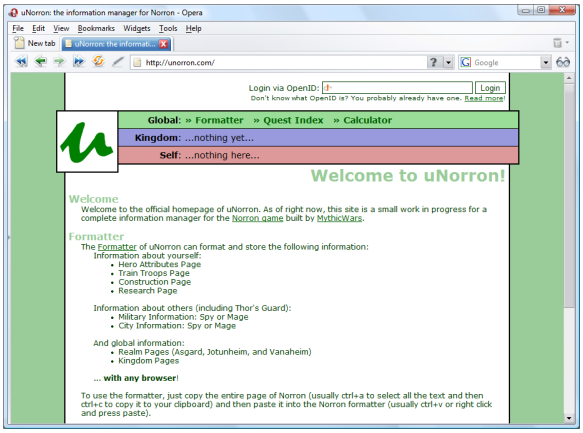

Figure 2: Screen shot of uNorron (http://unorron.com/), as seen by a user if arriving at uNorron for the first time.

Launched in late 2006, the massively multiplayer game (MMOG) Norron is a web-based strategy game that organizes players within fifty different kingdoms on a world map. Within Norron, each kingdom has a common communication area (an "assembly") that allows for the exchange of information but provides only basic forum functionalities. Therefore, the sharing of information between players within a kingdom is unnecessarily difficult given only the available resources in-game. Moreover, information is presented in-game as raw numbers (such as numbers of troops and buildings) rather than their actual values as the effect gameplay (such as offensive power and defensive power).

Figure 3: The orignal OpenID login box in uNorron.

Seeing the need for a more efficient means of communications, uNorron (http://uNorron.com/) was created as an information manager for Norron. The uNorron application is a completely web-based interface consisting of three main parts: the formatter, the attack calculator, and the quest index. The formatter allows for users to copy and paste their web browser from the Norron game into uNorron and the information is formatted for them in a meaningful way and stored on the uNorron server. Once information is imported into the uNorron formatter, users can choose a player to run the attack calculator on. The attack calculator calculates the results of an attack if the player chooses to attack the chosen target. Finally, the quest index simply outlines the tree of available quests to players. The quest index was added as an attraction to users of the site, and is not a part of the site particularly interesting to the study of OpenID.

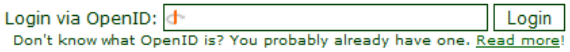

Figure 4: The improved OpenID login box in uNorron. The addition of a text to explain the OpenID process increased usage by over four fold.

Users may use the uNorron site without logging and will be able to store information about one target at a time. However, if a user logs in, the user then is able to store information about any number of targets. Moreover, a logged in user may associate themselves with a kingdom and share the target information with all users within a kingdom. To log in, a user simply logs in via OpenID though a textbox provided on the top-right corner of every uNorron page.

The initial design on the OpenID login box was a simple box that showed the text "Login via OpenID:" and provided an OpenID text box and a login button, as shown in Figure 3. Through analysis of the server logs, only two users (<3% of total unique IP addresses) successfully logged in through OpenID despite the added benefits. More surprisingly, six other users tried using what appeared to be a username in the OpenID box.

To counter the misinformed usage of OpenID, we modified the uNorron website with the text "Don't know what OpenID is? You probably already have one. Read More!". This modified login area can been seen in Figure 4. The "Read More" link directed users to a page explaining OpenID and linked them to OpenID identity providers. Within seven days, server logs indicate that successful logins via OpenID increased over four fold (11.7% of total unique IP addresses).

The uNorron project is an on going project that continues to expand in popularity as the world spreads within the Norron game about uNorron. In Section 5, we discuss the lessons learned by the uNorron application as well as the lessoned learned by the other implementations discussed in the next two sections.

4.2 FBOpenID

Introduced in Section 3.2, the concept of identity multiplexing allows for users to use any number of traditional Identity 1.0 identities as a means of authenticating any number of their Identity 2.0 identities that are supported by the site. To that end, FBOpenID (http://fbopenid.com/) was created to analyze user feedback and user reaction to a web service providing this type of identity multiplexing.

Specifically, FBOpenID provides users with the ability to login to their Facebook login through the Facebook API [13]. Once FBOpenID receives a positive

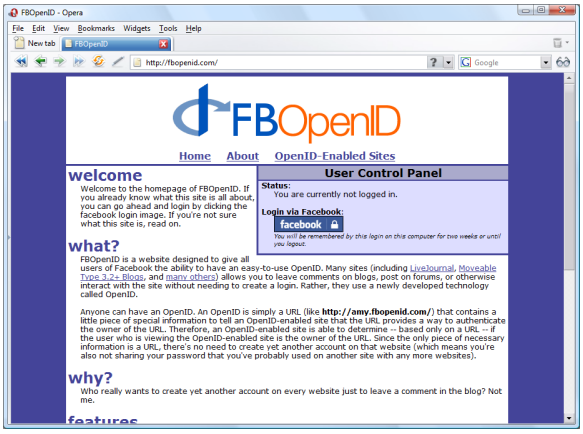

Figure 5: Screen shot of FBOpenID (http://fbopenid.com/), as seen by a user if arriving at FBOpenID for the first time.

assertion of the user's Facebook identity, the user is able to choose a subdomain of FBOpenID to be his or her identity. For example, the user Amy Smith could choose: "amy.fbopenid.com", "amy.smith.fbopenid.com", "gradschooler.fbopenid.com", or any other subdomain that hasn't been used by another user. Once the user has his or her subdomain, they may begin using it as either a login to sites supporting OpenID or to sites supporting Yadis.

Taking the lessons learned from uNorron, FBOpenID provided an explanation of both how the Facebook API will be securely authenticating their identity to us as well as how OpenID/Yadis will then allow them to securely log into any OpenID or Yadis-supporting site. Figure 5 shows a screenshot of the page a user would see upon visiting FBOpenID, with a description of the technology along site a login area in the top right corner of the context area.

Through informal user studies with fourteen users, where users were each given the link to FBOpenID and asked to play around with it and use it as they wish and could provide any feedback, the greatest concern of the users was the privacy of their identity. In fact, nearly half (six of fourteen users) raised concerns asking simular to: "how does an OpenID site know that someone else didn't type amy.fbopenid.com as my OpenID and login as me?" To attempt to counteract this fear, the addition of user-accessible logs showing all usage of their OpenID was provided for a user when they log in.

Based on another user's suggestion, this log was further modified to provide an always-visible "last used" status field on every page on FBOpenID when the user is logged in to show the user when he or she lasted used his or her FBOpenID. While not directly providing a more technical definition of the security of OpenID and Yadis, this was enough to have all but one of the six users to remark that this addition addressed their concern. We present a discussion on this and the other implementation projects with regard to the lessons we learned in Section 5.

4.3 MeIdentity

In our last of three projects, MeIdentity (http://meidentity.com/) presents a user-centric model of privacy designed for university or university-like setting. Unlike the previous implementations that were available for anyone to access on the Internet, MeIdentity was a prototype and was not able to interact with our university's authentication system to authenticate an OpenID based upon a student's university login. Instead, this prototype shows the ability to have differing levels of privacy based upon user locality and user preference.

Specifically, there are three different levels of security and identity privacy:

- User is on his or her personal IP address: The user needs only to provide a weak verification of identity (a short pin-number like number).
- User is on within his or her campus' IP address range: The user needs to provide a strong verification of identity (such as the student's university login).
- User is not within his or her campus' IP address range: The user needs to provide a strong verification of identity followed by a weak verification of identity.

Each of these levels of privacy are shown in Figure 6. Moreover, each user may choose to require a greater degree of authentication security at each level. For example, a user who's using his or her own IP address may know that they share their computer with a number of their friends commonly. Therefore, that user can choose to require a strong verification upon login even if they are on their own personal computer.

Of the fourteen users who viewed FBOpenID, twelve of them then viewed the MeIdentity prototype. Remarkably, every single user said they preferred this locality based authentication system over the authentication through Facebook. From this, we believe that as we filter more privacy control down to the user, we believe the user trusts the identity mechanism more and more. In the next section, we review the lessons we've learned through the three different implementations discussed in this and previous sections.

5. LESSONS LEARNED

In reviewing previous work, we found that the additional of single sign-on technologies has eased the authentication burden of the user and has been widely seen as a technology widely accepted by users. Specifically, we were unable to find anywhere that users were concerned about the security of their identity in cross-site authentication systems (such as when the .NET framework was used at third-party sites when Microsoft launched their single identity initiative). Instead, the greatest concern to users was reported to be the privacy of their information again and again.

With Identity 2.0 identity solutions being completely decentralized, a user can set up his or her own homesite and therefore control every aspect of the information his or her identity shares. By that inherit property, we thought that OpenID-based systems would show us results where users would have their individual concerns about specific aspects, but we didn't expect a strong overwhelming trend on a completely different issue. However, we found that users overwhelmingly were unsure of authentication schemes where the only information they provide to a site is a username.

Show in Figure 3 and Figure 4, an OpenID login box requests for the user to provide only a single piece of information to login. This process was counterintuitive to

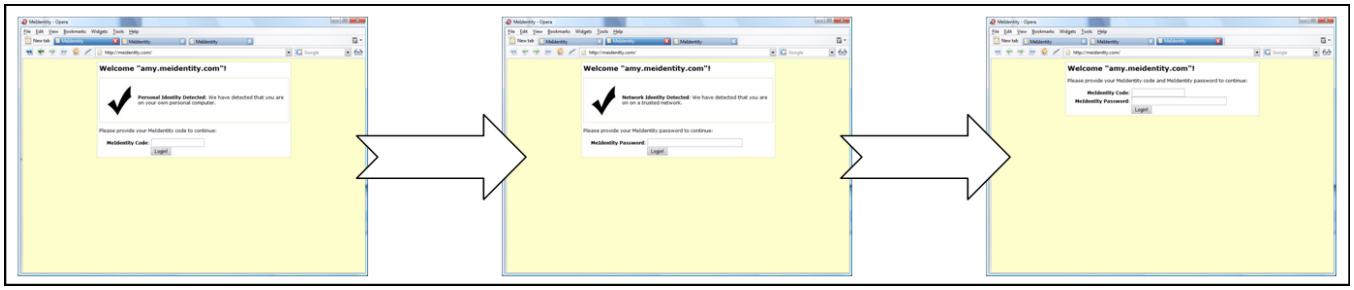

Figure 6: Three screen shots of the MeIdentity prototype in order of decreasing security. The first image (leftmost) shows a user coming from his or her personal IP address and needs only to provide their MeIdentity code. The next image (center) shows a user coming from within her trusted network (such as a university's IP range); this user would need only to provide their MeIdentity password. The last image (rightmost) shows a user coming from an untrusted network and was prompted to enter both his or her MeIdentity password and MeIdentity code. To prevent possible attacks from gathering any information, only minimal information about what is going on is provided to the user.

most users when they first saw the OpenID login box and, in uNorron, more users tried entering a username in the OpenID login box rather than a URL as an OpenID login box requires. It appears as though users are so used to logging in with both a username and a password that they are concerned for their privacy when they don't give a password to site. Therefore, we quickly learned that it is critical that, when a user is presented with authentication requiring anything less than a username and a password, a user is provided with a detailed description of how the technology works and how it ensures that someone can't type the same username and receive access to the user's information.

Going hand and hand with providing a description of technology to the user, we also found that users feel more secure with a technology when they are able to control the privacy of the technology. Existing literature suggests that privacy increases uses trust, but the correspondence seen between privacy and user's trust in applications of identity appears, based on initial results, to have a significantly stronger correlation. We assert that there's nothing more crucial to a user that his or her identity, and that a user would demand the most privacy controls with regard to his or her identity than nearly any other application. We back this assertion up with cases such as Facebook's introduction of the "News Feed", where media reports ran ramped with stories on users concerns over their privacy as all their actions were available for everyone to read and there were no privacy setting to limit the display of such information [16].

Therefore, we assert that there are two characteristics of user interaction discovered and supported by the work in this paper:

- *Login Security is Crucial*: Users generally feel insecure when they provide only a username to a site as a login credential. Any early adoption Identity 2.0 supporting technology will have to be sure to explain to end users how their information is secure and protected even though they appear to only provide a publicly available username.

- *Privacy Controls with Identity are Strongly Favored*: Users overwhelmingly favored a system where they were given the ability to control their privacy based on levels of access. We assert that while users generally appreciate privacy, this appreciation is strongest when it comes to the privacy of their very identity.

6. FUTURE WORK

The work is this paper is only the very beginning works toward understanding how users interact with Identity 2.0 identity solutions and what users will come to expect from identity management in the future. This paper presented an array of uses for identity technologies that provide for the a seamless user experience, but these technologies only touch the very tip of the iceberg of what's possibly with Identity 2.0 identity solutions.

In our work, we plan to continue the three projects presented in this paper: uNorron (http://unorron.com/), FBOpenID (http://fbopenid.com/), and MeIdentity (http://meidentity.com/). By introducing new features into uNorron slowly, we hope to understand if there becomes a point where a large amount of users choose that it's worthwhile to login using OpenID to receive additional features. Specifically, we're interested in seeing if there exists a well defined point between "very few users log in" to "very few users don't log in" - a bimodal distribution [4]. If such a point exists, it would provide valuable insight in what amount of content a sight ought to provide for a user to feel it's worthwhile to make their presence known if there are no other requirements (such as giving out an e-mail address, payment, or any other form of commitment).

We believe that coupling Identity 2.0 solutions with existing services could provide a new, richer experience for the user. For example, since Identity 2.0 identities are completely public, a user may wish to have disjoint identities while browsing on different parts of the Internet but have a site compile information for them about their combined identity. Many of these works begin to examine how the Internet might look with a wide-spread adoption of an Identity 2.0 solution.

Overall, we strongly believe that this field will be a field opening up to a large amount of industry-based and academic-based research. With the foundations already beginning to be seen of an Internet-wide Identity 2.0 solution in OpenID, we expect this to only spur the development of Identity 2.0 supporting applications able to make use of this interesting field of research.

7. CONCLUSION

In this paper, we began with the observation that nearly every site on the Internet requires a user to create "yet another identity" to make use of any meaningful customization on a given website. With users often using the same username and password combination to a number of the sites they've registered on, we found traditional identities to be insecure and site-centric rather than user-centric. These traditional identities, Identity 1.0 identity solutions, have dominated the Internet and have made it so that users expect to be required to provide both a username and a password to login to a site.

In contrast, Identity 2.0 identity solutions provide a decentralized user-centric model of identity that allows the user to control where he or she will store his or her own identity and the privacy policies behind it. In Section 3, we examine four interesting uses of Identity 2.0 identities that wasn't available using a traditional Identity 1.0 solution: greylisting, cross-site pre-registration, identity multiplexing, and user-centric privacy models. To understand many of these examples further, we developed two completely implementations that were deployed on the Internet for anyone to use: FBOpenID (http://fbopenid.com/) and uNorron (http://unorron.com). Moreover, a third application was developed as a prototype to understand user-centric privacy models: MeIdentity (http://meidentity.com/).

After examining server logs and informal user studies, we found two strong underlying trends in user's usage of Identity-based solutions: that users expect to provide a username and password to a site and that a user appreciates privacy when it comes to identity more so than a user appreciates privacy in other aspect of computer applications. To counter a user's concern about security and privacy when entering only a username to authenticate to a site, we found a detailed description of how their privacy and security is ensured appears to dampen a user's concern about their privacy and security. This was done as simply as adding a link to "Learn More" about OpenID below the OpenID login box.

Reflecting on what we found through our works, we briefly discuss our intentions to continue the projects introduced in this paper and discuss how we foresee research in Identity 2.0 based solutions will be an interesting and expanding area of research in the coming years. We strongly believe that Identity 2.0 solutions will make the Internet a more secure environment and allow users to control their identifies with a much greater degree of privacy, a desire that is reflected by a large number of users.

8. REFERENCES

[1] *Single sign-on systems-the technologies and the products*, 1995.

[2] *Single sign-on using cookies for Web applications*, 1999.

[3] *Security analysis of the SAML single sign-on browser/artifact profile*, 2003.

[4] K. P. Birman, M. Hayden, O. Ozkasap, Z. Xiao, M. Budiu, and Y. Minsky. Bimodal multicast. *ACM Trans. Comput. Syst.*, 17(2):41–88, 1999.

[5] D. Brickley and L. Miller. Foaf vocabulary specification, July 2005. http://xmlns.com/foaf/0.1/.

[6] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski. Computers beat humans at single character recognition in reading based human interaction proofs (hips). In *CEAS 2005: Second Conference on Email and Anti-Spam*, July 2006.

[7] M. Corporation. Windows cardspace. http://cardspace.netfx3.com/.

[8] S. I. Corporation. The sxip 2.0 protocol specification, 2006. http://sxip.net/index.php?title=Specs.

[9] E. Damiani, D. Capitani, and P. Samarati. Managing multiple and dependable identities. *IEEE Internet Computing*, 7(6):29–37, 2003.

[10] J. Ernst. Light weight identity (lid), 2005. http://lid.netmesh.org/.

[11] S. C. et al. Assertions and protocols for the oasis security assertion markup language (saml) v2.0, oasis standard, March 2005. http://docs.oasis-open.org/security/saml/v2.0/samlcore-2.0-os.pdf.

[12] S. Garriss, M. Kaminsky, M. J. Freedman, B. Karp, D. Mazires, and H. Yu. Re: Reliable email. In *In Proceedings of the 3rd Symposium on Networked Systems Design and Implementation (NSDI 06)*, pages 297–310, May 2006.

[13] F. Inc. Facebook platform 1.0. http://developers.facebook.com/.

[14] N. Johnston. Mythicwars: Norron. http://mythicwars.com/norron/default.asp.

[15] W. K. Josephson, E. G. Sirer, and F. B. Schneider. *Peer-to-Peer Authentication with a Distributed Single Sign-On Service*. 2005.

[16] B. Mazzola, 2006. http://media.www.bsudailynews.com/media/storage/paper849/news/2006/09/06/News/Facebook.news.Feed.Upsets.Angers.Students.Across.Country-2258118.shtml.

[17] J. Miller. Yadis 1.0, March 2006. http://yadis.org/papers/yadisv1.0.pdf.

[18] R. Oppliger. Microsoft .net passport: a security analysis. *Computer*, 36(7):29–35, 2003.

[19] B. Pfitzmann and M. Waidner. Analysis of liberty single-sign-on with enabled clients. *Internet Computing, IEEE*, 7(6):38–44, 2003.

[20] D. Recordon and B. Fitzpatrick. Openid authentication 1.1, May 2006. http://www.openid.net/specs/openidauthentication-1_1.txt.

[21] D. Recordon and D. Reed. Openid 2.0: a platform for user-centric identity management. In *DIM '06: Proceedings of the second ACM workshop on Digital identity management*, pages 11–16, New York, NY, USA, 2006. ACM Press.

[22] A. Volchkov. Revisiting single sign-on: a pragmatic approach in a new context. *IT Professional*, 3(1):39–45, 2001.

[23] S. Willison. Social whitelisting with openid, January 2007. http://simonwillison.net/2007/Jan/22/whitelisting/.

[24] K. Y-N. How to hack a quarter of all japanese web users accounts, August 2006. http://whatjapanthinks.com/2006/08/08/how-to-hack-a-quarter-of-all-japanese-web-users-accounts/.

[25] G. Zhao, D. Zheng, and K. Chen. Design of single sign-on. In *IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04)*, pages 253–256, 2004.